IN THE SPECIFICATION:

1. Please replace the full paragraph starting on line 13 of specification page 3, with the following replacement paragraph:

Current ~~ant-pirate~~anti-pirating software methods within the art function as follows with a few minor twists. After the application is stored and executed onto the user's computer, the user will be provided with a generated parameter. The user is prompted to contact the vendor to exchange this parameter for a key. The user then enters the key into the system, which stores it into a hidden place(s). Some methods encrypt the key, and some do not. Some hide the key in many places, and some do not. Subsequent executions of the application verify that the key is found. If the key is not found, the user is denied access. The idea is that if the application is moved to another computer, the hidden key is not transferred. Therefore, on execution, the key is not found and access is denied. Such methods rely on authenticating registered users merely by detecting keys placed onto their system, and not authenticating the user's computer itself. Such methods suffer from the following limitations and problems, these methods are: 1) insufficiently secure, 2) the security level is static, and 3) not user-friendly for the user. In general, this is because of several drawbacks common to known anti-pirate software methods.

2. Please replace the full paragraph starting on line 28 of specification page 3 over to page 4 with the following replacement paragraph:

First, current methods rely on discriminating registered users from non-registered users by placing known values on the registered user's system—and not on discriminating a user's system itself from other systems. Second, current methods do not repeatedly authenticate the user's system itself—much less once—as the user requests access to the application. Third, current methods have an architecture that does not allow for the some functionality to be performed, at the user's system, before the application is stored onto

the user's system. This leads to several security risks, such as, the inability to ensure that the protected application is only sent to registered users in the first place. Furthermore, the current architecture makes it difficult, if not impossible, for these methods to have dynamic capabilities. Thus, security can not be ~~individual tailed~~individually tailored for each particular computer, but in fact is the same for any computer. Therefore, with current methods, a hacker may more easily develop and publish an application that will pirate any so enabled application on any computer. Finally, current methods do not have functionality that is invisible to the user—making such methods not user-friendly.

3. Please replace the full paragraph starting on line 21 of specification page 7 with the following replacement paragraph:

An individual becomes a 'user' of the protected application by completing a ~~monitory~~ monetary transaction and/or executing a license agreement. After this (these) transaction (s) the server application imprints the client application with a sales number or similar transition parameter (Fig. 1) sufficient to uniquely identify that particular license event. The client application is then delivered to the user via email, a download, or by physical means such as on a compact or floppy disk.